

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-160876

(43)Date of publication of application : 20.06.1997

(51)Int.Cl. G06F 15/00  
G06F 13/00  
G06F 15/16

(21)Application number : 08-229538

(71)Applicant : INTERNATL BUSINESS MACH CORP &lt;IBM&gt;

(22)Date of filing : 30.08.1996

(72)Inventor : KELLS TIMOTHY ROGER  
PEEBLES THOMAS FRANK

(30)Priority

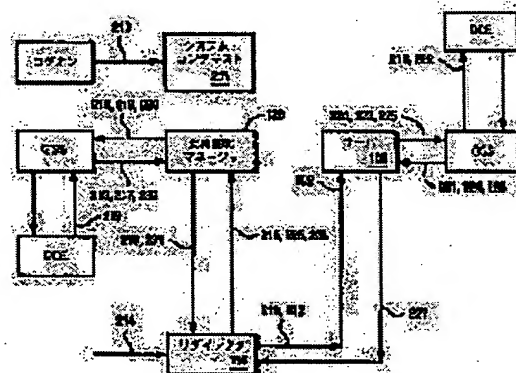
Priority number : 95 570463 Priority date : 11.12.1995 Priority country : US

## (54) METHOD AND DEVICE FOR MUTUAL CONFIRMATION IN LAN SERVER ENVIRONMENT

(57)Abstract:

**PROBLEM TO BE SOLVED:** To support decentralized computer mechanisms in LAN server environment by enabling the LAN server machine of a computerized LAN network to pass a generic name security subsystem (GSS) decentralized computer environment (DCE) qualification certificate by making use of an existent mechanism.

**SOLUTION:** A user logs on first (210) and a log-in context is set as a system context (211). Then an LSCred MGR function acquires the qualification certificate of the user (212) and a GSS qualification certificate is generated from the system context (213). Then a session setup request to the server is generated (214). In a series of steps 215-218, the context token of the server including a GSS call to DCE is acquired. Thus, the LAN server can hand down the qualification certificate by making use to the existent mechanism.



## LEGAL STATUS

[Date of request for examination] 28.07.1998

[Date of sending the examiner's decision of rejection] 15.04.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection] 2003-12954

[Date of requesting appeal against examiner's decision of rejection] 09.07.2003

[Date of extinction of right]

(11)特許出願公開番号

特開平9-160876

(43)公開日 平成9年(1997)6月20日

(51) Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0		G 0 6 F 15/00	3 3 0 A
13/00	3 5 7		13/00	3 5 7 Z
15/16	3 7 0		15/16	3 7 0 N

審査請求 未請求 請求項の数24 O.L (全 14 頁)

(21) 出願番号	特願平8-229538	(71) 出願人	390009531 インターナショナル・ビジネス・マシーンズ・コーポレーション INTERNATIONAL BUSINESS MACHINES CORPORATION アメリカ合衆国10504、ニューヨーク州 アーモンク (番地なし)
(22) 出願日	平成8年(1996)8月30日	(72) 発明者	ティモシー・ロジャー・ケルス アメリカ合衆国78681、テキサス州ラウンド・ロック、グレイリング・レーン 3919
(31) 優先権主張番号	08/570463	(74) 代理人	弁理士 合田 潔 (外2名)
(32) 優先日	1995年12月11日		
(33) 優先権主張国	米国 (US)		

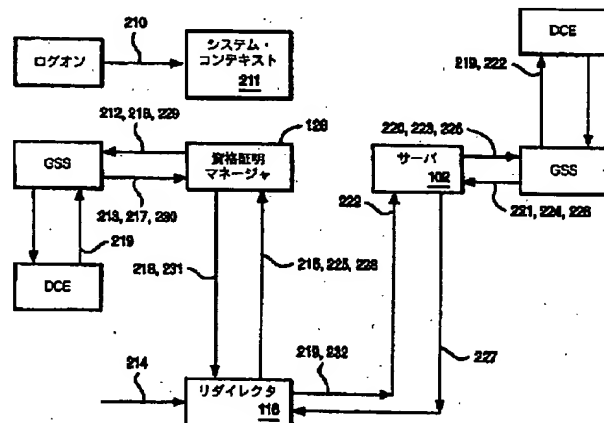
**最終頁に続く**

(54) 【発明の名称】 LANサーバ環境における相互確認の方法及び装置

(57)【要約】

【課題】 LANサーバ環境において分散コンピュータ機構をサポートする。

【解決手段】 LANサーバが、既存の機構を利用して、総称セキュリティ・サブシステム（GSS）DCE資格証明を渡すことができるように構成される。サーバ管理ブロック（SMB）プロトコルが拡張され、サーバはGSS API インタフェースを用いて資格証明を獲得及び確認する。GSSインタフェースが、クライアントとサーバ間で相互確認を達成するために必要な全ての情報をカプセル化するトークンを提供する。こうしたSMBプロトコル拡張に関して、折衝プロトコル（NP）SMBにより交換される新たなプロトコル名を含む新たなプロトコル・レベルが定義される。既存のLANサーバがNP応答内のSMB\_secmodeフィールドのビットをオンし、サーバがsecpkgX SMBの交換をサポートすることを示す。サーバは次にSMBsecpkgXまたはSMBsesssetupX要求を待機する。



## 【 特許請求の範囲】

【請求項1】遠隔プロシジャ呼び出しを元来サポートしないローカル・エリア・ネットワーク・サーバ環境において相互接続されるクライアントとサーバとの間で、分散コンピュータ環境(DCE)資格証明により、セッション・セットアップの間の相互確認を改良する方法であって、

資格証明を交換するためのサーバ管理ブロック(SMB)・プロトコルの拡張を事前定義するステップと、前記サーバにより、総称セキュリティ・サブシステム(GSS)を前記事前定義済み拡張の機能として、前記分散コンピュータ環境により定義される総称セキュリティ・サブシステムAPIインタフェースを通じてアクセスするステップと、前記アクセスに回答して、前記総称セキュリティ・サブシステムから前記資格証明を獲得し、確認するステップと、を含む、方法。

【請求項2】前記アクセスするステップが、前記クライアント及び前記サーバにより、前記相互確認を実行するために必要な情報をカプセル化するトークンを取り出すステップを含む、請求項1記載の方法。

【請求項3】前記サーバ管理ブロック・プロトコルの拡張が、折衝プロトコル応答内のSMB\_secmodeフィールド内の第2ビットを活動化するステップを含む、請求項2記載の方法。

【請求項4】前記サーバにより、SMBsecpkgx応答を検出するステップと、前記検出に回答して、前記クライアントと前記サーバとの間で、前記相互確認を達成するための総称セキュリティ・サブシステム・トークンを交換するステップと、を含む、請求項3記載の方法。

【請求項5】前記SMBsecpkgx応答に対応する総称セキュリティ・サブシステム/分散コンピュータ環境トークン・パッケージを定義するステップを含む、請求項4記載の方法。

【請求項6】前記クライアントにより、前記サーバに送信する第1のトークンを獲得するためのGSS\_initiate\_sec\_context機能と呼び出すステップと、前記クライアントからの前記第1のトークンに回答して、前記GSS\_initiate\_sec\_context機能に第2のトークンを転送するステップと、前記GSS\_initiate\_sec\_context機能により、前記サーバが確認されたか否かを返却するステップと、を含む、請求項5記載の方法。

【請求項7】前記SMBsecpkgx応答の検出に回答して、前記サーバにより前記第2のトークンを抽出するステップと、GSS\_accept\_sec\_context機能により、前記抽出されたトークンを処理するステップと、

クライアント確認に回答して、前記サーバにより、前記クライアントに送信する総称セキュリティ・サブシステム・トークンを受信するステップと、

前記SMBsecpkgx応答にもとづき、前記総称セキュリティ・サブシステム・トークンを前記クライアントに転送するステップと、

前記サーバにより、前記総称セキュリティ・サブシステム・トークンから前記ユーザの資格証明を抽出するステップと、

10 前記クライアントが前記ネットワークの資源へのアクセスを探索するときのために、前記抽出された資格証明をセッション・データ構造に付加するステップと、を含む、請求項6記載の方法。

【請求項8】前記サーバがリダイレクタを含み、前記リダイレクタ及び前記総称セキュリティ・サブシステムが異なるリングで動作し、前記方法が、資格証明マネージャ・プロセスを、前記リダイレクタと前記総称セキュリティ・サブシステムとの間の媒介として確立するステップを含む、

20 請求項7記載の方法。

【請求項9】遠隔プロシジャ呼び出しを元来サポートしないローカル・エリア・ネットワーク・サーバ環境において相互接続されるクライアントとサーバとの間で、分散コンピュータ環境(DCE)資格証明によりセッション・セットアップの間の相互確認を改良する装置であって、

資格証明を交換するためのサーバ管理ブロック(SMB)・プロトコルの拡張を事前定義する手段と、前記サーバにより、総称セキュリティ・サブシステム(GSS)を前記事前定義済み拡張の機能として、前記分散コンピュータ環境により定義される総称セキュリティ・サブシステムAPIインタフェースを通じてアクセスする手段と、前記アクセスに回答して、前記総称セキュリティ・サブシステムから資格証明を獲得し、確認する手段と、を含む、装置。

【請求項10】前記アクセスする手段が、前記クライアント及び前記サーバにより、前記相互確認を実行するために必要な情報をカプセル化するトークンを取り出す手段を含む、請求項9記載の装置。

30 【請求項11】前記サーバ管理ブロック・プロトコルの前記拡張のための手段が、折衝プロトコル応答内のSMB\_secmodeフィールド内の第2ビットを活動化する手段を含む、請求項10記載の装置。

【請求項12】前記サーバにより、SMBsecpkgx応答を検出する手段と、

前記検出に回答して、前記クライアントと前記サーバとの間で、前記相互確認を達成するための総称セキュリティ・サブシステム・トークンを交換する手段と、

50 を含む、請求項11記載の装置。

3

【請求項1 3】前記SMBsecpkgx応答に対応する総称セキュリティ・サブシステム／分散コンピュータ環境トークン・パッケージを定義する手段を含む、請求項1 2記載の装置。

【請求項1 4】前記クライアントにより、前記サーバに送信する第1のトークンを獲得するためのGSS\_initiate\_sec\_context機能を呼び出す手段と、前記クライアントからの前記第1のトークンにตอบสนองして、前記GSS\_initiate\_sec\_context機能に第2のトークンを転送する手段と、

前記GSS\_initiate\_sec\_context機能により、前記サーバが確認されたか否かを返却する手段と、を含む、請求項1 3記載の装置。

【請求項1 5】前記SMBsecpkgx応答の検出にตอบสนองして、前記サーバにより前記第2のトークンを抽出する手段と、

GSS\_accept\_sec\_context機能により、前記抽出されたトークンを処理する手段と、

クライアント確認にตอบสนองして、前記サーバにより、前記クライアントに送信する総称セキュリティ・サブシステム・トークンを受信する手段と、

前記SMBsecpkgx応答にもとづき、前記総称セキュリティ・サブシステム・トークンを前記クライアントに転送する手段と、

前記サーバにより、前記総称セキュリティ・サブシステム・トークンから前記ユーザの資格証明を抽出する手段と、

前記クライアントが前記ネットワークの資源へのアクセスを探索するするときのために、前記抽出された資格証明をセッション・データ構造に付加する手段と、

を含む、請求項1 4記載の装置。

【請求項1 6】前記サーバがリダイレクタを含み、前記リダイレクタ及び前記総称セキュリティ・サブシステムが異なるリングで動作し、前記装置が、資格証明マネージャ・プロセスを、前記リダイレクタと前記総称セキュリティ・サブシステムとの間の媒介として確立する手段を含む、

請求項1 5記載の装置。

【請求項1 7】遠隔プロシジャ呼び出しを元来サポートしないローカル・エリア・ネットワーク・サーバ環境において相互接続されるクライアントとサーバとの間で、分散コンピュータ環境(DCE)資格証明によりセッション・セットアップの間の相互確認を改良するためのコンピュータ・プログラム製品であって、資格証明を交換するためのサーバ管理ブロック(SMB)・プロトコルの拡張を事前定義するコンピュータ読出し可能プログラム・コード手段と、

前記サーバにより、総称セキュリティ・サブシステム(GSS)を前記事前定義済み拡張の機能として、前記分散コンピュータ環境により定義される総称セキュリテ

4

ィ・サブシステムAPIインタフェースを通じてアクセスするコンピュータ読出し可能プログラム・コード手段と、

前記アクセスにตอบสนองして、前記総称セキュリティ・サブシステムから資格証明を獲得し、確認するコンピュータ読出し可能プログラム・コード手段と、を含む、コンピュータ・プログラム製品。

【請求項1 8】前記アクセスするコンピュータ読出し可能プログラム・コード手段が、前記クライアント及び前記サーバにより、前記相互確認を実行するために必要な情報をカプセル化するトークンを取り出すコンピュータ読出し可能プログラム・コード手段を含む、請求項1 7記載のコンピュータ・プログラム製品。

【請求項1 9】前記サーバ管理ブロック・プロトコルの拡張のための前記コンピュータ読出し可能プログラム・コード手段が、折衝プロトコル応答内のSMB\_secmodeフィールド内の第2ビットを活動化するコンピュータ読出し可能プログラム・コード手段を含む、請求項1 8記載のコンピュータ・プログラム製品。

【請求項2 0】前記サーバにより、SMBsecpkgx応答を検出するコンピュータ読出し可能プログラム・コード手段と、

前記検出にตอบสนองして、前記クライアントと前記サーバとの間で、前記相互確認を達成するための総称セキュリティ・サブシステム・トークンを交換するコンピュータ読出し可能プログラム・コード手段と、を含む、請求項1 9記載のコンピュータ・プログラム製品。

【請求項2 1】前記SMBsecpkgx応答に対応する総称セキュリティ・サブシステム／分散コンピュータ環境トークン・パッケージを定義するコンピュータ読出し可能プログラム・コード手段を含む、請求項2 0記載のコンピュータ・プログラム製品。

【請求項2 2】前記クライアントにより、前記サーバに送信する第1のトークンを獲得するためのGSS\_initiate\_sec\_context機能を呼び出すコンピュータ読出し可能プログラム・コード手段と、

前記クライアントからの前記第1のトークンにตอบสนองして、前記GSS\_initiate\_sec\_context機能に第2のトークンを転送するコンピュータ読出し可能プログラム・コード手段と、

前記GSS\_initiate\_sec\_context機能により、前記サーバが確認されたか否かを返却するコンピュータ読出し可能プログラム・コード手段と、を含む、請求項2 1記載のコンピュータ・プログラム製品。

【請求項2 3】前記SMBsecpkgx応答の検出にตอบสนองして、前記サーバにより前記第2のトークンを抽出するコンピュータ読出し可能プログラム・コード手段と、

GSS\_accept\_sec\_context機能により、前記抽出されたト

50

5

ークンを処理するコンピュータ 読出し 可能プログラム・コード 手段と、

クライアント 確認に 応答して、前記サーバにより、前記クライアント に送信する総称セキュリティ・サブシステム・トークンを受信するコンピュータ 読出し 可能プログラム・コード 手段と、

前記SMBsecpkix 応答にもとづき、前記総称セキュリティ・サブシステム・トークンを前記クライアント に転送するコンピュータ 読出し 可能プログラム・コード 手段と、前記サーバにより、前記総称セキュリティ・サブシステム・トークンから前記ユーザの資格証明を抽出するコンピュータ 読出し 可能プログラム・コード 手段と、前記クライアント が前記ネットワークの資源へのアクセスを探索するするときのために、前記抽出された資格証明をセッション・データ構造に付加するコンピュータ 読出し 可能プログラム・コード 手段と、を含む、請求項22 記載のコンピュータ・プログラム製品。

【請求項24】前記サーバがリダイレクタを含み、前記リダイレクタ及び前記総称セキュリティ・サブシステムが異なるリングで動作し、前記コンピュータ・プログラム製品が、資格証明マネージャ・プロセスを、前記リダイレクタと前記総称セキュリティ・サブシステムとの間の媒介として確立するコンピュータ 読出し 可能プログラム・コード 手段を含む、請求項23 記載のコンピュータ・プログラム製品。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はコンピュータ・システムにおける確認(authentication)に関し、特に、クライアント-サーバ・ローカル・エリア・ネットワーク(LAN)環境における確認技術に関する。

【0002】

【従来の技術】通常のLANにおけるセッションのセットアップでは、プロセスが従来通り発散し、図2に示されるように、クライアント-ユーザ100及びサーバ102がネットワーク・プロトコル104(NP)を折衝する。こうした折衝の間、プロトコル及び関連するプロトコル・レベル208が合意され(例えばCORE、LAN 2.1などに対応)、セッション・キー106がクライアント100に対して決定される。

【0003】クライアント-ユーザ100は通常、ユーザID、名前、及びパスワードなどの情報112をサーバ102に、より詳細には、リダイレクタ116(図5)に伝送する。これはLANサーバ102への(からの)ネットワーク・インタフェースとして機能する。リダイレクタ116は本来、ネットワーク・インタフェース、ディスク・ドライブの再転送(redirecting)、及びファイル入出力などの目的を果たす。例えばクライ

6

アントがドライブに接続する場合、クライアントにとってそれはローカル・ドライブと思われるかも知れない。しかしながら、リダイレクタは本来、ドライブを管理する実際のファイル・システムにドライブ指定を渡し得るファイル・システムとして機能することにより、要求をクライアントから、ドライブを処理する実際のファイル・サーバに再転送する。こうしたプロセスはクライアントには透過的である。

【0004】従来の動作では、サーバ102が通常、次にそのデータベース118(図3)を調査し、ユーザIDにもとづき、ユーザのパスワード及びセッション・キー106(図2)を抽出し、一致が存在したか否かを判断する。存在した場合、サーバ102はサーバのローカル・データベース118からユーザ定義120(図3)をフェッチする。このセッション・キー106は本来、タイムスタンプまたは通し番号である。ここでの技法では、本発明の説明の中で明らかとなる理由から、データベース118を使用するのではなく、分散コンピュータ環境(DCE: Distributed Computing Environment)及び関連するカベロス・レジストリ(Kerberos registry)122(図4)を使用し、より詳細には、ユーザ定義が内在するDCEのディレクトリ及びセキュリティ・サーバ(DSS)・コンポーネントを使用する。

【0005】要するに、クライアント100は分散コンピュータ環境にログオンするとき、プロトコル104(図2)を折衝し、その結果、プロトコル・レベル208が返却される。IBMのLANサーバ・エンタープライズ(LSE)製品などの、DCEを使用する特定のLANサーバ環境では、DCEの利用を確認し、従ってLANに接続するユーザであるためのDCE資格証明(credentials)を関連付けることが望ましい。なぜなら、これは通常のLANサーバ確認機構によるよりも、相当に安全な環境であると思われるからである。従って、ログオン時に、サーバ102が理解し得るDCE資格証明を獲得することが望ましく、こうしたDCE資格証明は通常、遠隔プロシジャ呼び出し(RPC)を通じて獲得される。

【0006】しかしながら、クライアント100からサーバ102にこうしたDCE資格証明を獲得する機構が提供されないLANでは、問題が生じ得ることが判明している。より詳細には、例えばLSE及び類似のLAN製品では、元来RPC呼び出しが利用されないにも関わらず、サーバはセッションのセットアップの間に、ユーザを確認するために、真正の資格証明を獲得する必要がある。こうした資格証明は、POSIXアクセス制御リスト(ACL)により保護されるLSE資源へのアクセスを決定するために使用される。

【0007】

【発明が解決しようとする課題】従って、従来のLANサーバ機構を利用する一方で、現プロトコルによりクラ

7

クライアントからサーバに、こうしたDCE 資格証明を獲得する機構を提供する重大な問題が提示される。こうした現プロトコルには、例えばサーバ管理ブロック ( S M B ) ・プロトコルなど、通常X/Open協会により定義されるものが含まれる。

【 0 0 0 8 】

【課題を解決するための手段】本発明の好適な実施例では、コンピュータ化LANネットワーク内のLANサーバ・マシンが、それらの既存の機構を利用して、総称セキュリティ・サブシステム ( G S S : generic security subsystem ) 分散コンピュータ環境 ( D C E ) 資格証明を渡すことができるように構成される。X/Openにより定義されるサーバ管理ブロック ( S M B ) ・プロトコルが、こうした資格証明の交換を容易にするように拡張される。サーバはDCEにより提供されるGSS API インタフェースを用いて、こうした資格証明を獲得及び確認する。GSSインタフェースは、クライアントとサーバ間で相互確認を達成するために必要な全ての情報をカプセル化するトークンを提供する。

【 0 0 0 9 】好適な実施例では、こうしたSMBプロトコル拡張に関して新たなプロトコル・レベルが定義され、これは特定の実施例では、折衝プロトコル ( N P : negotiate protocol ) SMBにより交換される新たなプロトコル名を含む。I B M LANサーバ・エンタープライズ ( L S E ) 製品などの既存のLANサーバは、応答内のSMB\_secmodeフィールドのビット ( L S Eに関するビット 2 ) をオンし、こうしたビットは、サーバがsecpkgX SMBの交換をサポートすることを示す。サーバは次にSMBsecpkgXまたはSMBsesssetupX要求を待機する。前者の応答は、ユーザ/クライアント及びサーバがGSSトークンを交換し、相互に確認することを可能にし、更に、サーバが複数のパッケージから選択することを可能にする。既存のLANサーバ製品は、新たなパッケージをSMB\_pkgnameの名で定義し、LANサーバはこれをGSS DCEトークンを処理するために送信及び認識する。クライアント上のユーザは、SMBsecpkgXが伝送されたとき確認される。なぜなら、確認は、サーバがユーザを追跡するために必要なデータ構造を割り当て、返却するからである。

【 0 0 1 0 】更に本発明によれば、GSSトークンの処理に関して、クライアント側において、クライアントがサーバに送信するトークンを獲得するためにgss\_initiate\_sec\_context機能が呼び出される。トークンがサーバに送信され、戻りトークンがサーバから受信される。戻りトークンが次にgss\_initiate\_sec\_context機能に渡され、これが次にサーバが確認されたか否かを返却する。サーバが確認されない場合、セッションの確立が終了される。

【 0 0 1 1 】サーバ側では、SMBsecpkgX応答が受信されるとき、トークンがgss\_accept\_sec\_context機能により

8

抽出され、処理される。クライアントが確認されると、クライアントに送信するためのトークンも受信される。トークンはSMBsecpkgX応答により、クライアントに送信される。SMBを送信後、サーバはユーザの資格証明をGSSトークンから抽出する。資格証明がセッションのデータ構造に付加され、その後、ユーザが資源をアクセスしようとする度に利用される。

【 0 0 1 2 】リダイレクターGSS間インタフェースに関して、ここで開示される好適な実施例では、LANサーバ・リダイレクタは通常、リング0で実行され、GSSはリング3で実行される。このことは、リダイレクタ及びGSSが直接通信し得ないことを意味する。従って、本発明によれば、資格証明マネージャ・プロセスが媒介として生成される。資格証明マネージャは、起動時にリダイレクタに専用の ( captive ) スレッドを提供する。LANサーバへの接続が形成されるとき、リダイレクタは専用スレッドを用いてGSSトークンを要求し、処理する。資格証明マネージャは、LANサーバに現在ログオンされているユーザの資格証明を用いてトークンを獲得する。ユーザ・プロファイル管理 ( U P M ) プロセスは、資格証明マネージャにログオン及びログオフ事象を通知する。これは資格証明マネージャが、セッションのセットアップ試行の度に、U P Mに問い合わせること無く、ログオン・ユーザを追跡することを可能にする。

【 0 0 1 3 】

【発明の実施の形態】最初に図1を参照して、本発明が好適に実現され得るネットワーク環境について説明する。図1は、本発明の方法及びシステムを実現するために使用され得るデータ処理システム8を絵的に表している。図示のように、データ処理システム8はLAN10及びLAN32などの複数のネットワークを含み、各々のLANは、好適には複数の個々のコンピュータ12、12a乃至12c、30、31、33及び35を含む。(以下、ネットワーク32内のコンピュータについて述べる場合、コンピュータ30を任意に参照するが、説明はネットワーク32内の任意のコンピュータに当てはまる。)コンピュータ12及び30は、例えばI B Mパーソナル・システム/2 ( "P S / 2 "とも呼ばれる ) ・コンピュータまたはI B M RISC SYSTEM/6000コンピュータ・ワークステーションなどの、任意の好適なコンピュータを用いて実現される。ここで "RISC SYSTEM/6000"はI B Mの商標であり、"パーソナル・システム/2"及び"P S / 2 "はI B Mの登録商標である。もちろん、当業者には理解されるように、ホスト・プロセッサに接続される複数の高機能ワークステーション ( I W S ) が、こうした各ネットワークにおいて使用され得る。

【 0 0 1 4 】こうしたデータ処理システムにおいて一般的なように、各個々のコンピュータは記憶装置14及び ( または ) プリンタ/出力装置16に接続される。本発

明の方法によれば、1 つ以上のこうした記憶装置1 4 が、文書、資源オブジェクト、または実行可能コードなどのオブジェクトを記憶するために使用され、これらのオブジェクトは、データ処理システム8 内の任意のユーザにより周期的にアクセスされ得る。既知のようにして、記憶装置1 4 内のこうした各オブジェクトは、オブジェクトを例えば個々のコンピュータ1 2 または3 0 のユーザに転送することにより、データ処理システム8 を通じて自由に交換され得る。

【0015】更に図1 を参照すると、データ処理システム8 はメインフレーム・コンピュータ1 8 などの、複数のメインフレーム・コンピュータを含むことが分かる。これらは、好適には通信リンク2 2 によりLAN1 0 に接続される。メインフレーム・コンピュータ1 8 は、IBMから提供されるエンタープライズ・システム・アーキテクチャ/3 7 0 ( "ESA/3 7 0 "とも呼ばれる)、またはエンタープライズ・システム・アーキテクチャ/3 9 0 ( "ESA/3 9 0 "とも呼ばれる) コンピュータを用いて実現され得る。アプリケーションに依存して、例えばアプリケーション・システム/4 0 0 ( "AS/4 0 0 "とも呼ばれる) などの、中型コンピュータも使用され得る。"エンタープライズ・システム・アーキテクチャ/3 7 0 "、"ESA/3 7 0 "、"エンタープライズ・システム・アーキテクチャ/3 9 0 "、及び"ESA/3 9 0 "は、IBMの商標であり、"アプリケーション・システム/4 0 0 "及び"AS/4 0 0 "は、IBMの登録商標である。メインフレーム・コンピュータ1 8 は更に、LAN1 0 の遠隔記憶装置として機能し得る記憶装置2 0 にも接続され得る。同様に、LAN1 0 は通信リンク2 4 、更にサブシステム制御ユニット/通信制御装置2 6 及び通信リンク3 4 を通じて、ゲートウェイ・サーバ2 8 に接続され得る。ゲートウェイ・サーバ2 8 は好適には、LAN3 2 をLAN1 0 にリンクする機能を果たす個々のコンピュータまたはI WS である。

【0016】LAN3 2 及びLAN1 0 に関連して上述したように、オブジェクトは記憶装置2 0 内に記憶され、記憶されたオブジェクトのための資源マネージャまたはファイル・システム・マネージャとしてのメインフレーム・コンピュータ1 8 により制御され得る。もちろん、当業者には、メインフレーム・コンピュータ1 8 がLAN1 0 から地理的に遠く離れて配置されてもよく、同様にLAN1 0 がLAN3 2 から遠く離れて配置され得ることが理解されよう。例えば、LAN3 2 がカルフォルニア州に配置され、LAN1 0 がテキサス州に配置され、メインフレーム・コンピュータ1 8 がニューヨーク州に配置されたりする。

【0017】本発明の好適な実施例は、データ処理システム8 内に示される様々なコンピュータに組み込まれ得る。

【0018】DCEの一部であるDSS プロトコルでは、クライアント1 0 0 ( 図2 ) がレジストリ1 2 2 ( 図4 ) にチケットを要求し、これが次にサーバ1 0 2 ( 図2 ) に渡される。幾つかのアプリケーションでは、図7 の1 2 4 で示されるようなネット利用( NetUse ) をリダイレクタ1 1 6 に発行し、これがプロトコルを開始する。すなわち、本来、ユーザ発行コマンドがクライアント1 0 0 をトリガし、サーバ1 0 2 とのセッションをセットアップする。このネット利用にตอบสนองして、リダイレクタ1 1 6 は、プロトコル及びセッション・セットアップの折衝のために、X/OpenのS MB 通信プロトコルに従い、サーバ管理ブロック( S MB ) を発行する。しかしながら、本発明によれば、DCEの総称セキュリティ・サブシステム( GSS ) ・コンポーネント1 2 6 ( 図7 ) 、及び前述の図7 の1 1 6 で示されるリダイレクタを利用するLANサーバにおいて、要求を資格証明マネージャ1 2 8 を通じてGSS 1 2 6 に伝達する機構を提供する問題が提示される。この機構を実現するために、資格証明マネージャ1 2 8 に対して状態マシン( 図8 ) が定義される。なぜなら、セッションをセットアップするために、資格証明マネージャとリダイレクタとの間でコマンドが交換されるからである。この状態マシンの動作は、図8 に関連して以下で詳述される。

【0019】X/Openプロトコルにより定義されるS MB は、本来、ユーザを確認するために使用される機構であるパッケージの概念を提供する自由形式のセキュリティ拡張である。固有のこうしたパッケージが、図7 の1 3 0 などのトークンの受け渡しを提供する本技法において定義されることは、本発明の重要な特徴である。更に図7 を参照すると、このトークン1 3 0 はGSS 1 2 6 から資格証明マネージャ1 2 8 に、そして次にリダイレクタ1 1 6 に渡されるように示される( 図6 にも示される)。ここで、リダイレクタ1 1 6 が本来クライアントのコンポーネントであることが思い起こされよう。サーバはこのトークン1 3 0 がGSS パッケージとして受信された後に、これを処理するために、gss\_accept\_context呼び出し1 3 3 ( 図6 ) を発行する。リダイレクタによるトークンの受信は、サーバ1 0 2 に第2 のトークン1 3 2 ( 図6 ) を獲得するように指示する。クライアント1 0 0 が次にこの第2 のトークン1 3 2 を資格証明マネージャ1 2 8 に、続いてGSS 1 2 6 転送し、この時GSS がサーバ1 0 2 を確認する。

【0020】要するに、第1 のトークンがネットワークを通じて転送されるとき、クライアントは本来、それ自身をサーバに証明済みである。証明されていない場合、セッションのセットアップは終了し、一方、証明されている場合には、セッションのセットアップが実行される。サーバは既にクライアントを確認済みであるので、サーバは機能呼び出しをGSS 1 2 6 に発行し、前述のように、定義をユーザのGSS から獲得する。従来のシ

システムでは、前述のように、ユーザを確認するためのユーザ定義120を獲得するために、サーバがそれら自身のデータベース(図3の参照番号118で示される)を保守した。しかしながら、本発明によれば、GSSがあらゆるサーバに対して複製されず、また異なるセキュリティ機構がGSSの下で提供され得る。DCE拡張によりシステムは資格証明を獲得でき、ユーザが確認されるだけでなく、本システムによればユーザを確認したサーバを知ることができる。GSSが使用されるが、確認のために実際に下位で使用されるのは、DCE内のカペロス機能である。

【0021】要するに、ここではDCEにより統合される従来のLANサーバ・ワークステーション及びサーバが、それらの既存の機構を用いて、確認のためにGSS DCE資格証明を受け渡すことを可能にするシステムが開示される。ここで開示される特定の実施例では、IBMから提供されるOS/2(商標)オペレーティング・システムを実行するワークステーション及びサーバに対して、変更が成されるが、本発明はこれに限るものではない。代表的なLANシステムに関する詳細については、"OS/2 Lan Server, Programming Guide and Reference"(著作権IBM, S10H-9687-00, 1994)を参照されたい。しかしながら、上述の概念は、他のオペレーティング・システムを実行するワークステーション及びサーバにも拡張され得る。

【0022】OS/2の実施例では、既存のLANサーバ製品に対する変更が、NP応答内のsmb\_secmodeフィールドの第2ビットをオンする。サーバは次に前述のSMBsecpkgXまたはSMBsesssetupX要求を待機する。前者はもちろん、ユーザ及びサーバがGSSトークンを交換し、相互に確認し合うことを可能にし、これについてはX/Open社から提供される"PROTOCOLS FOR X/OPEN PC INTERWORKING: SMB VERSION 2", Section 11.2で定義されている。この機能は、サーバが複数のパッケージから選択することを可能にする。

【0023】SMBsecpkgX要求に続くSMBsesssetupX要求は、長さ0のsmb\_apasswdを有し得る。なぜなら確認が既に発生しており、その中のあらゆる内容が無視されるからである。SMBsecpkgX要求が受信されないか、SMBsec

pkgX要求内に既知のパッケージが含まれないで受信された場合、smb\_apasswdフィールドは、サーバがユーザを確認するための有効パスワードを含まねばならない。この場合、サーバはユーザの資格証明を獲得しなければならない。

【0024】ここで述べられる本発明の実施例によれば、折衝プロトコルが次のように変更されなければならない。secpkgX(上述のsecmodeフィールドのビット番号2)をイネーブルするために、セット・フラグが生成される。更に、サーバがレガシ・クライアント(legacy client)をサポートするか否かを決定する新たなsrvhueristicビットが提供される。レガシ・サポートがオフの場合、サーバは折衝時に、レガシ・プロトコルのセットを提供しない。このことは安全性が不確かなレガシ・クライアントの接続を阻止する。

【0025】更に前述のように、新たなプロトコル・レベルが定義され、これは特定の技法では、ストリングLSE10がワイヤー上を流れることを規定する。クロスセル・サーバのチケットを獲得するために、NP応答がサーバのセル名及びその長さを含むように変化する。セル名はドメイン名の後に置かれ、セキュリティ・コンテキストを獲得するときに資格証明マネージャ128(図5)により使用される。セル名はクロスセル確認のために要求されるが、折衝がLSE10ストリングに帰着するときのみ送信される。

【0026】また前述のように、secpkgXの変化が要求される。この機能はX/Open社から提供される前記"PROTOCOLS FOR X/OPEN PC INTERWORKING: SMB VERSION 2", Section 11.2で定義されている。このフォーマットはここで開示される実施例において使用され、特定の情報が例えばIBMから提供されるLS4.0Eなどの、使用される特定のLANサーバのために定義される。SMBpkglist構造では、SMB\_pkgnameが"LANサーバ4.0E GSS/DCEトークン"であり、これは前述のように、LS4.0Eサーバ製品が送信または認識する唯一のパッケージである。

【0027】下記の表では、前述のSMBsecpkgXのデータ構造が、次のように定義される。

【表1】

Request Format:

```

BYTE  smb_ccm;          /* 値=7E (????) */
BYTE  smb_wct;          /* 値=4 */
BYTE  smb_ccm2;         /* 2次(X)コマンド、0xFF=none */
BYTE  smb_reh2;         /* 予約(0でなければならない) */
WORD   smb_off2;        /* (SMBヘッダ開始から)次のコマンド(@smb_wct) */
                               /* へのオフセット */
WORD   smb_pkgtype;     /* パッケージ・タイプ=0 */
WORD   smb_numpkge;     /* リスト内のパッケージ数 */
WORD   smb_bcc;
struct smb_pkglist[*];  /* パッケージ・リスト構造。LS4.0Eの1パッケージ・リスト */

```



Package List Structure (smb\_pkglist) Format:

```
WORD  smb_pkgnamlen; /* パッケージ名の長さ */
WORD  smb_pkgarglen; /* パッケージ特有情報の長さ */
BYTE  smb_pkgname[*]; /* パッケージ名 */
struct smb_pkgargs[1]; /* LS4.0Eのパッケージ特有情報 */
```

Package Specific Information (smb\_pkgargs) Format:

```
DWORD smb_xp_flags; /* ビット - セットされると、GSSTークンを伴う応答が */
/* 相互確認のために要求される */
WORD  smb_xp_TokenLen; /* GSSTークンの長さ */
BYTE  smb_xp_Token[*]; /* 確認情報を含むGSSTークン */
BYTE  smb_xp_name[*]; /* 確認されるユーザ名 */
```

Response Format:

```
BYTE  smb_com; /* 値=7E */
BYTE  smb_wct; /* 値=4 */
BYTE  smb_com2; /* 2 次 (X)コマンド、0xFF=none */
BYTE  smb_reh2; /* 予約 ( 0 でなければならない ) */
WORD  smb_off2; /* ( SMBヘッダ 開始から ) 次のコマンド ( @smb_wct ) */
/* へのオフセット */
WORD  smb_index; /* サーバにより選択されるパッケージの番号。 */
/* LS4.0Eでは0 */
WORD  smb_pkgarglen; /* パッケージ特有情報の長さ */
WORD  smb_bcc;
struct smb_pkgargs[1]; /* パッケージ特有情報 */
```

Package Specific Information (smb\_pkgargs) Format:

```
DWORD smb_xp_flags; /* ビット0、GSSTークンが別の一巡の交換を要求。 */
BYTE  smb_xp_Token[*]; /* 確認情報を含むGSSTークン */
```

【 0 0 2 8 】図5 を参照すると、本システムの基本フローが図式的に示される。最初に、ユーザがログオンし ( 2 1 0 )、ログイン・コンテキストがシステム・コンテキストとしてセットされる ( 2 1 1 )。次に、LS4.0E 30 MCR機能がユーザの資格証明を獲得し ( 2 1 2 )、GS S 資格証明がシステム・コンテキストから生成される ( 2 1 3 )。続いて、サーバへのセッション・セットアップ要求が生成される ( 2 1 4 )。次の一連のステップ 2 1 5 乃至 2 1 8 は、DCE への GSS 呼び出しを含むサーバのコンテキスト・トークンが獲得されることを表す。

【 0 0 2 9 】次にステップ 2 1 9 で、システム・コンテキスト・トークンを含む SMBsecpkg\_x 呼び出しが送信される。この時点で、サーバは始動時の資格証明を獲得し ( 2 2 0、2 2 1 )、SMBsecpkg\_x が受信される ( 2 2 2 )。次にステップ 2 2 3、2 2 4 で、サーバは GSS\_Accept\_context 機能によりユーザを確認し、DCE への GSS 呼び出しを含む応答 トークンを受信する。続いてステップ 2 2 5、2 2 6 で、サーバは GSS トークンから EPAC を抽出する。次に、GSS コンテキスト・トークンを含む SMBsecpkg\_x 応答が送信され、受信される ( 2 2 7 )。次にステップ 2 2 8 乃至 2 3 1 により示されるように、DCE への GSS 呼び出しを含むサーバのコンテキスト・トークンが確認される。最後に、ステッ 50

プ 2 3 2 により示されるように、SMBsessSetup\_x が送信され、受信される。

【 0 0 3 0 】本発明の別の面は、有限のライフタイムを有するトークンを提供する従来の実施例に関連する。トークンが消滅するとき、通常、サーバは自動的にクライアントとの接続を切断する。従って、トークンを周期的にリフレッシュするための特定の手段が必要とされる。

【 0 0 3 1 】本発明によれば、セッションがセットアップされた後、資格証明マネージャ 1 2 8 ( 図 5 ) が、チケットの残りのライフタイムを判断する。消滅の直前に、こうした判断を実施した後、資格証明マネージャ 1 2 8 は好適には新たなトークンを獲得し、それをサーバ 1 0 2 に転送する。このトークンは図 6 のトークン 2 4 2 として表され、図 8 の状態マシンにより提供される事象モニタリング機能に関連して、詳細に後述される。

【 0 0 3 2 】現ログオン・ステータスは、資格証明マネージャ 1 2 8 がどのようにコンテキストを管理するかに影響する。本来、次に示すように、資格証明マネージャに影響する 4 つのログオン事象が存在する。

【 0 0 3 3 】第 1 は、図 8 に示されるように、ログオン機能 2 3 8 である。資格証明マネージャ 1 2 8 は、DCE システム資格証明を獲得しなければならない。資格証明はログオン実行からインポートされる。次に、ログオフ事象 2 3 6 が同様に、資格証明マネージャ 1 2 8 に影

15

響する。資格証明マネージャは、ログオン・ユーザのために保持していた全てのセッション情報をクリアしなければならない。ログオフが発生するとき、リダイレクタが全てのセッションをクローズし、使用しているDCEシステム資格証明を解放する。この事象はクリーンアップ及び状態保守のためにも必要とされる。第3に、資格証明リフレッシュ234が上述のように提供される。この事象は、資格証明マネージャが資格証明を消滅された状態に移転することを阻止する。資格証明キャッシュ名は変化しない。システムが既に消滅状態の場合、新たなコンテキスト及びキャッシュ名が獲得される。資格証明マネージャは両方のタイプのリフレッシュを処理する。第4に、図8の参照番号240で示されるように、資格証明の消滅が状態マシンに提供される。資格証明が消滅すると、資格証明マネージャ128はもはやチケットを獲得できない。資格証明マネージャ128は従って、この状態の間に要求が到来すると、エラー・コードをリダイレクタに返却する。ユーザがこの状態になると、資格証明はリフレッシュされ得ずに、新たな資格証明のセットがログオン実行により獲得される。

【0034】資格証明マネージャ128の別の面は、クライアント100がシャットダウンされるときに言及されるべきである。こうした事象において、リダイレクタ116はこれ(例えばネット停止機能)を検出し、その時、リダイレクタ116により発行されるクローズ・コマンド(図7の260)が、資格証明マネージャ・プロセス128を終了させる。システムが再始動されるとき、リダイレクタ116はブートに際して明らかに開始される。しかしながら、資格証明マネージャ128はGSSの残りが開始されるまで、依然実行されない。GSSが開始すると、資格証明マネージャ128はトークン・コマンド130を送信し、これはリダイレクタ116内で専用(captive)に保持される。この実行スレッドは次にリダイレクタにより使用され、リダイレクタは接続1コマンド262を発行する。接続2コマンド264は、スレッドを資格証明マネージャ128内において専用に保持する。

【0035】前述の説明を考慮し、ここで述べられる本発明の技法の追加のファクタは、注目に値する。DCE用語では、"資格証明(credentials)"はカペロス・チケット、またはより総称的には、ユーザ及びグループの定義と見なされ得る。ユーザは例えば管理者、ゲスト、ユーザなどのメンバである。こうした資格証明は通常、1プロセス当たりを基本とし(on a per process basis)、各プロセスはいわばそれ自身のプロセスを管理する責任を託される。しかしながら、本発明によれば、資格証明マネージャが、個々のプロセスを管理する全てのネットワーク・システムとして提供される。従って本発明によれば、全てのこうした個々のプロセスは、前記項目の責任が、通常例えば特定のログインの使用のよう

16

に、プロセス特有であると見なされると想定する限り、DCE資格証明がそれらの下で動作していることを考えない。通常、これはアプリケーション毎に固有である。しかしながら本発明によれば、プロセス特有のアプリケーションが様々な呼び出しをするとき、それらがシステム・レベル・ベースで管理され、資格証明マネージャは各々のプロセスが何であるかを知り、トークンを獲得するために適切な資格証明を送信する。

【0036】本発明によれば、セキュリティを管理する比較的異類の機構を実現した2つのソフトウェア・エンティティが、本質的に併合される。より詳細には、本発明はDCEコードと共に既存の機構を利用するLANサーバ・マシンを提供し、それにより、従来のLANのこれら2つのエンティティ及びDCEコードが、継ぎ目無く作用するようにまとめられる。セキュリティのLAN技法が比較的単純な確認を提供し、そして本発明によるDCE確認を使用する利点の1つが、より複雑な確認機構により、より安全な環境を提供することによることが思い起こされよう。

【0037】LANサーバがGSS DCE資格証明と共に動作することを可能にする資格証明マネージャ技法の新規の提供に加え、X/Open仕様及びSMBアーキテクチャの一部であるSMBsecpkgXパッケージを使用する本発明のトークンの技法は、新規の結果を提供する。本発明のこの面によれば、定義される新規のパッケージが、相互確認を示すフラグ、前述のトークン、並びにユーザ名を含む。ユーザ名は、通常、ユーザが定義されるセッション・セットアップ時に、後のSMB内で獲得される。SMBsecpkg\_Xがセッション・セットアップ時に使用する確認プロトコルの折衝であるのではなく、本発明によれば、確認がセッション・セットアップから上流のSMBsecpkg\_X機能に移される。

【0038】その体系的な定義により、セッション・セットアップにおいて、ユーザが確認される。しかしながら、本発明によれば、上述のように確認がSMBより以前に移される。従って、システムがセッション・セットアップに至るとき、セッション・セットアップを達成する作業が実行されるが、確認は要求されない。なぜなら、確認は既に達成されているからである。カスタムSMBsecpkg\_Xパッケージの新規の使用を通じて確認が効果的に、あるSMBから別のSMBに移される。しかしながら、このパッケージ機能の従来の利用は、製品がセッション・キーにより暗号化されて送信されるときであり、本発明の特徴は、確認のための異なる機構(例えば異なる暗号化アルゴリズム、キーなど)の指定を所望通りに可能にする。しかしながら本発明の技法は、前述のように、確認をセッション・セットアップから上流のSMBsecpkg\_Xパッケージの伝送に移すことを容易にする。

【0039】本発明は特定の実施例に関連して述べられてきたが、当業者には、本発明の趣旨及び範囲から逸脱

すること無しに、その形態及び詳細における他の変更が可能であることが理解されよう。

【 0 0 4 0 】 まとめとして、本発明の構成に関して以下の事項を開示する。

【 0 0 4 1 】 ( 1 ) 遠隔プロシジャ呼び出しを元来サポートしないローカル・エリア・ネットワーク・サーバ環境において相互接続されるクライアントとサーバとの間で、分散コンピュータ環境 ( DCE ) 資格証明により、セッション・セットアップの間の相互確認を改良する方法であって、資格証明を交換するためのサーバ管理ブロック ( S M B ) ・プロトコルの拡張を事前定義するステップと、前記サーバにより、総称セキュリティ・サブシステム ( G S S ) を前記事前定義済み拡張の機能として、前記分散コンピュータ環境により定義される総称セキュリティ・サブシステムAPI インタフェースを通じてアクセスするステップと、前記アクセスに回答して、前記総称セキュリティ・サブシステムから前記資格証明を獲得し、確認するステップと、を含む、方法。

( 2 ) 前記アクセスするステップが、前記クライアント及び前記サーバにより、前記相互確認を実行するために必要な情報をカプセル化するトークンを取り出すステップを含む、前記 ( 1 ) 記載の方法。

( 3 ) 前記サーバ管理ブロック・プロトコルの拡張が、折衝プロトコル応答内のSMB\_secnodeフィールド内の第2ビットを活動化するステップを含む、前記 ( 2 ) 記載の方法。

( 4 ) 前記サーバにより、SMBsecpkgx応答を検出するステップと、前記検出に回答して、前記クライアントと前記サーバとの間で、前記相互確認を達成するための総称セキュリティ・サブシステム・トークンを交換するステップと、を含む、前記 ( 3 ) 記載の方法。

( 5 ) 前記SMBsecpkgx応答に対応する総称セキュリティ・サブシステム/分散コンピュータ環境トークン・パッケージを定義するステップを含む、前記 ( 4 ) 記載の方法。

( 6 ) 前記クライアントにより、前記サーバに送信する第1のトークンを獲得するためのGSS\_initiate\_sec\_context機能を呼び出すステップと、前記クライアントからの前記第1のトークンに回答して、前記GSS\_initiate\_sec\_context機能に第2のトークンを転送するステップと、前記GSS\_initiate\_sec\_context機能により、前記サーバが確認されたか否かを返却するステップと、を含む、前記 ( 5 ) 記載の方法。

( 7 ) 前記SMBsecpkgx応答の検出に回答して、前記サーバにより前記第2のトークンを抽出するステップと、GSS\_accept\_sec\_context機能により、前記抽出されたトークンを処理するステップと、クライアント確認に回答して、前記サーバにより、前記クライアントに送信する総称セキュリティ・サブシステム・トークンを受信するステップと、前記SMBsecpkgx応答にもとづき、前記総称セ

キュリティ・サブシステム・トークンを前記クライアントに転送するステップと、前記サーバにより、前記総称セキュリティ・サブシステム・トークンから前記ユーザの資格証明を抽出するステップと、前記クライアントが前記ネットワークの資源へのアクセスを探索するときのために、前記抽出された資格証明をセッション・データ構造に付加するステップと、を含む、前記 ( 6 ) 記載の方法。

( 8 ) 前記サーバがリダイレクタを含み、前記リダイレクタ及び前記総称セキュリティ・サブシステムが異なるリングで動作し、前記方法が、資格証明マネージャ・プロセスを、前記リダイレクタと前記総称セキュリティ・サブシステムとの間の媒介として確立するステップを含む、前記 ( 7 ) 記載の方法。

( 9 ) 遠隔プロシジャ呼び出しを元来サポートしないローカル・エリア・ネットワーク・サーバ環境において相互接続されるクライアントとサーバとの間で、分散コンピュータ環境 ( DCE ) 資格証明によりセッション・セットアップの間の相互確認を改良する装置であって、資格証明を交換するためのサーバ管理ブロック ( S M B ) ・プロトコルの拡張を事前定義する手段と、前記サーバにより、総称セキュリティ・サブシステム ( G S S ) を前記事前定義済み拡張の機能として、前記分散コンピュータ環境により定義される総称セキュリティ・サブシステムAPI インタフェースを通じてアクセスする手段と、前記アクセスに回答して、前記総称セキュリティ・サブシステムから資格証明を獲得し、確認する手段と、を含む、装置。

( 1 0 ) 前記アクセスする手段が、前記クライアント及び前記サーバにより、前記相互確認を実行するために必要な情報をカプセル化するトークンを取り出す手段を含む、前記 ( 9 ) 記載の装置。

( 1 1 ) 前記サーバ管理ブロック・プロトコルの前記拡張のための手段が、折衝プロトコル応答内のSMB\_secnodeフィールド内の第2ビットを活動化する手段を含む、前記 ( 1 0 ) 記載の装置。

( 1 2 ) 前記サーバにより、SMBsecpkgx応答を検出する手段と、前記検出に回答して、前記クライアントと前記サーバとの間で、前記相互確認を達成するための総称セキュリティ・サブシステム・トークンを交換する手段と、を含む、前記 ( 1 1 ) 記載の装置。

( 1 3 ) 前記SMBsecpkgx応答に対応する総称セキュリティ・サブシステム/分散コンピュータ環境トークン・パッケージを定義する手段を含む、前記 ( 1 2 ) 記載の装置。

( 1 4 ) 前記クライアントにより、前記サーバに送信する第1のトークンを獲得するためのGSS\_initiate\_sec\_context機能を呼び出す手段と、前記クライアントからの前記第1のトークンに回答して、前記GSS\_initiate\_sec\_context機能に第2のトークンを転送する手段と、前記

GSS\_initiate\_sec\_context機能により、前記サーバが確認されたか否かを返却する手段と、を含む、前記(13)記載の装置。

(15) 前記SMBsecpkix応答の検出にตอบสนองして、前記サーバにより前記第2のトークンを抽出する手段と、GSS\_accept\_sec\_context機能により、前記抽出されたトークン进行处理する手段と、クライアント確認にตอบสนองして、前記サーバにより、前記クライアントに送信する総称セキュリティ・サブシステム・トークンを受信する手段と、前記SMBsecpkix応答にもとづき、前記総称セキュリティ・サブシステム・トークンを前記クライアントに転送する手段と、前記サーバにより、前記総称セキュリティ・サブシステム・トークンから前記ユーザの資格証明を抽出する手段と、前記クライアントが前記ネットワークの資源へのアクセスを探索するするときのために、前記抽出された資格証明をセッション・データ構造に付加する手段と、を含む、前記(14)記載の装置。

(16) 前記サーバがリダイレクタを含み、前記リダイレクタ及び前記総称セキュリティ・サブシステムが異なるリングで動作し、前記装置が、資格証明マネージャ・プロセスを、前記リダイレクタと前記総称セキュリティ・サブシステムとの間の媒介として確立する手段を含む、前記(15)記載の装置。

(17) 遠隔プロシジャ呼び出しを元来サポートしないローカル・エリア・ネットワーク・サーバ環境において相互接続されるクライアントとサーバとの間で、分散コンピュータ環境(DCE)資格証明によりセッション・セットアップの間の相互確認を改良するためのコンピュータ・プログラム製品であって、資格証明を交換するためのサーバ管理ブロック(SMB)・プロトコルの拡張を事前定義するコンピュータ読出し可能プログラム・コード手段と、前記サーバにより、総称セキュリティ・サブシステム(GSS)を前記事前定義済み拡張の機能として、前記分散コンピュータ環境により定義される総称セキュリティ・サブシステムAPIインタフェースを通じてアクセスするコンピュータ読出し可能プログラム・コード手段と、前記アクセスにตอบสนองして、前記総称セキュリティ・サブシステムから資格証明を獲得し、確認するコンピュータ読出し可能プログラム・コード手段と、を含む、コンピュータ・プログラム製品。

(18) 前記アクセスするコンピュータ読出し可能プログラム・コード手段が、前記クライアント及び前記サーバにより、前記相互確認を実行するために必要な情報をカプセル化するトークンを取り出すコンピュータ読出し可能プログラム・コード手段を含む、前記(17)記載のコンピュータ・プログラム製品。

(19) 前記サーバ管理ブロック・プロトコルの拡張のための前記コンピュータ読出し可能プログラム・コード手段が、折衝プロトコル応答内のSMB\_secmodeフィールド内の第2ビットを活動化するコンピュータ読出し可能

プログラム・コード手段を含む、前記(18)記載のコンピュータ・プログラム製品。

(20) 前記サーバにより、SMBsecpkix応答を検出するコンピュータ読出し可能プログラム・コード手段と、前記検出にตอบสนองして、前記クライアントと前記サーバとの間で、前記相互確認を達成するための総称セキュリティ・サブシステム・トークンを交換するコンピュータ読出し可能プログラム・コード手段と、を含む、前記(19)記載のコンピュータ・プログラム製品。

(21) 前記SMBsecpkix応答に対応する総称セキュリティ・サブシステム/分散コンピュータ環境トークン・パッケージを定義するコンピュータ読出し可能プログラム・コード手段を含む、前記(20)記載のコンピュータ・プログラム製品。

(22) 前記クライアントにより、前記サーバに送信する第1のトークンを獲得するためのGSS\_initiate\_sec\_context機能と呼び出すコンピュータ読出し可能プログラム・コード手段と、前記クライアントからの前記第1のトークンにตอบสนองして、前記GSS\_initiate\_sec\_context機能に第2のトークンを転送するコンピュータ読出し可能プログラム・コード手段と、前記GSS\_initiate\_sec\_context機能により、前記サーバが確認されたか否かを返却するコンピュータ読出し可能プログラム・コード手段と、を含む、前記(21)記載のコンピュータ・プログラム製品。

(23) 前記SMBsecpkix応答の検出にตอบสนองして、前記サーバにより前記第2のトークンを抽出するコンピュータ読出し可能プログラム・コード手段と、GSS\_accept\_sec\_context機能により、前記抽出されたトークン进行处理するコンピュータ読出し可能プログラム・コード手段と、クライアント確認にตอบสนองして、前記サーバにより、前記クライアントに送信する総称セキュリティ・サブシステム・トークンを受信するコンピュータ読出し可能プログラム・コード手段と、前記SMBsecpkix応答にもとづき、前記総称セキュリティ・サブシステム・トークンを前記クライアントに転送するコンピュータ読出し可能プログラム・コード手段と、前記サーバにより、前記総称セキュリティ・サブシステム・トークンから前記ユーザの資格証明を抽出するコンピュータ読出し可能プログラム・コード手段と、前記クライアントが前記ネットワークの資源へのアクセスを探索するするときのために、前記抽出された資格証明をセッション・データ構造に付加するコンピュータ読出し可能プログラム・コード手段と、を含む、前記(22)記載のコンピュータ・プログラム製品。

(24) 前記サーバがリダイレクタを含み、前記リダイレクタ及び前記総称セキュリティ・サブシステムが異なるリングで動作し、前記コンピュータ・プログラム製品が、資格証明マネージャ・プロセスを、前記リダイレクタと前記総称セキュリティ・サブシステムとの間の媒介

21

として確立するコンピュータ読出し可能プログラム・コード手段を含む、前記( 2 3 ) 記載のコンピュータ・プログラム製品。

【 図面の簡単な説明】

【 図1 】 本発明が有利に採用され得るコンピュータ・ネットワークの機能ブロック図である。

【 図2 】 プロトコル折衝を図式的に示す図である。

【 図3 】 ユーザ定義を獲得するための、サーバによるデータベースの利用を示す図である。

【 図4 】 ユーザ定義を獲得するための、サーバによるDCEレジストリの利用を示すブロック図である。

【 図5 】 図1 のシステムにおいて実現可能な本発明のコンポーネント及び信号フローを示すブロック図である。

【 図6 】 本発明のトークン機構を図式的に示す図である。

22

【 図7 】 本発明の資格証明マネージャ及びリダイレクタを示すブロック図である。

【 図8 】 本発明により採用される状態マシンを示す図である。

【 符号の説明】

8 データ処理システム

1 2、1 2 a、1 2 b、1 2 c、3 0、3 1、3 3、3

5 コンピュータ

1 4、2 0 記憶装置

1 6 プリンタ/出力装置

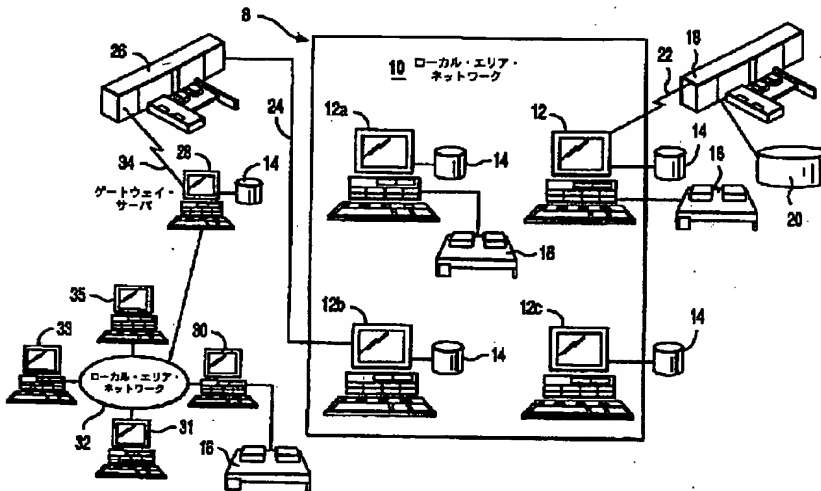
1 8 メインフレーム・コンピュータ

2 2、2 4、3 4 通信リンク

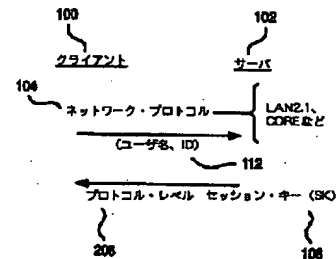
2 6 サブシステム制御ユニット/通信制御装置

1 1 8 データベース

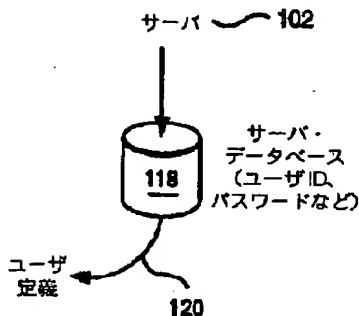
【 図1 】



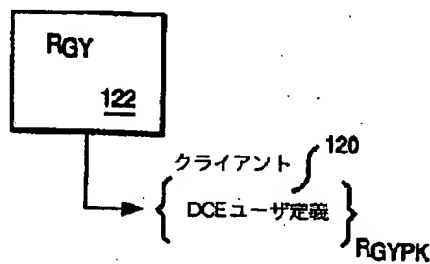
【 図2 】



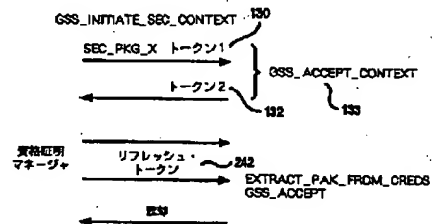
【 図3 】



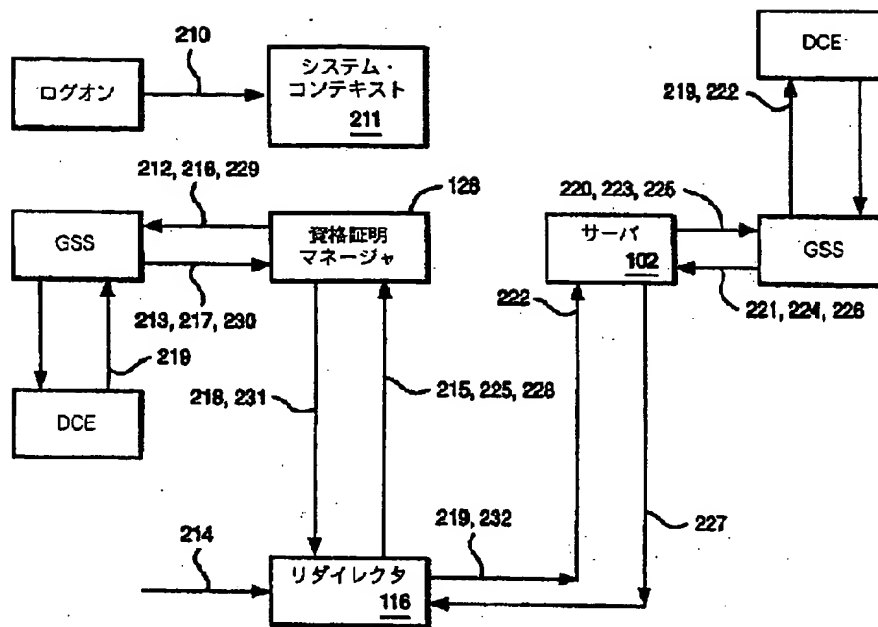
【 図4 】



【 図6 】



【 図5 】



【 図8 】

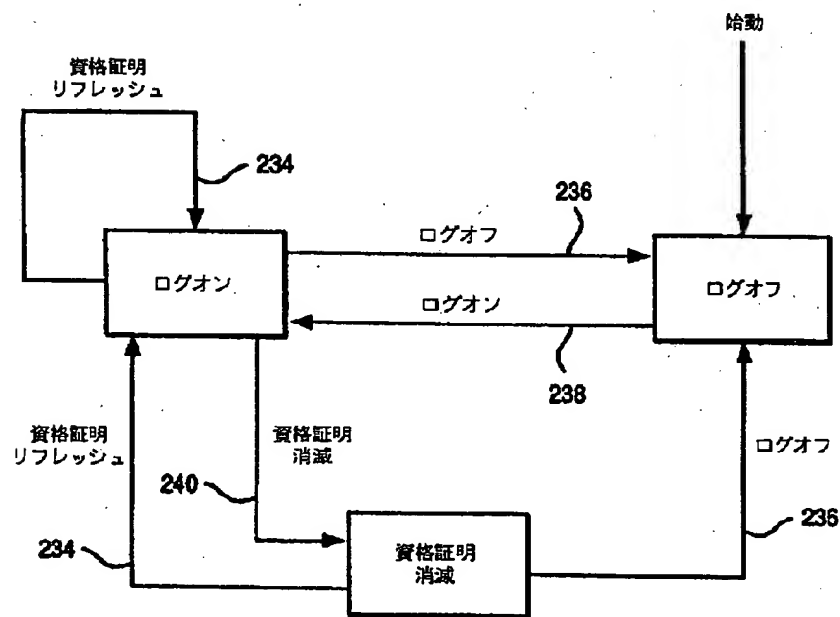


Figure 1 consists of two diagrams illustrating network configurations and operations.

The upper diagram shows a network topology divided into two rings by a dashed line labeled "リング0" (Ring 0). Above the line is "リング3" (Ring 3). Components include:

- アプリケーション・ネット利用** (Application Network Use) connected to the Ring 3 side.
- 資格証明マネージャ 128** (Credential Manager 128) connected to both Ring 3 and Ring 0.
- GSS (DCE) 126** connected to the Credential Manager 128.
- リダイレクタ 116** (Redirector 116) connected to the Ring 0 side.

Connections and flows are labeled:

- トークン1 130** (Token 1 130) between GSS 126 and Credential Manager 128.
- 接続1 262** (Connection 1 262) and **接続2 264** (Connection 2 264) between Credential Manager 128 and Redirector 116.
- クローズ 280** (Close 280) from Redirector 116 to Credential Manager 128.
- トークン1 130** (Token 1 130) from Credential Manager 128 to Redirector 116.
- ネット利用 124** (Network Use 124) from Application Network Use to Redirector 116.

The lower diagram shows an operation flow:

- ログオン** (Logon) box at the top.
- 資格証明マネージャ 128** (Credential Manager 128) below it.
- リダイレクタ 116** (Redirector 116) at the bottom.

Flow steps are indicated by arrows and text:

- ネット開始** (Network Start) from Logon to Credential Manager 128.
- ネット停止** (Network Stop) from Credential Manager 128 to Logon.
- ブート** (Boot) from Credential Manager 128 to Redirector 116.
- A dashed line labeled **R0** separates the Credential Manager 128 from the Redirector 116.

(72)発明者 トーマス・フランク・ピーブルズ  
アメリカ合衆国78758、テキサス州オース  
ティン、ソーンワイルド・パス 2323